B2B PAYMENTS

The Lasting Impact Of Corporates' Mistrust Of The Cloud

By PYMNTS

Posted on October 2, 2017

Cloud-based systems were met with **heavy skepticism** from corporates only a few years ago. That skepticism has largely waned, though, with many organizations taking a hybrid approach to cloud solutions and, eventually, entrusting the cloud to store key information like financial data.

But that early skepticism has had some long-lasting consequences. Mainly, large enterprises that weren't ready to implement cloud-based ERP systems instead decided to have top providers like Oracle and SAP develop customized, on-premise solutions. According to Mike Whitmire, co-founder and CEO of **FloQast**, the ongoing use of in-house ERP systems comes with its own set of difficulties and pain points.

FloQast launched in 2013 as a firm providing other businesses with software to help them close their books every month or quarter. When the company began, Whitmire told PYMNTS, it was during that period of distrust of the cloud.

"Within the finance and accounting world, there seemed to be general resistance to the cloud, mainly circulated around security," he said. "Putting financial data in the cloud [could] be perceived as a major security risk."

Since the company launched, businesses are now more open to the idea of putting financial data in the cloud, though. For up-and-coming, innovative companies, that means an easy decision to implement a cloud-based ERP.

"For companies that have been around a while and already implemented an SAP or an Oracle, they've just put too many resources [into] getting that in place," Whitmire explained. "It takes a lot of time and money, and the idea of switching over to any other ERP, regardless of whether it's [on-premise] or in the cloud, is a daunting concept. The trouble of switching over is not worth the benefits they'll get from adopting the cloud at that point."

The Trouble With Data

On-premise ERP systems may provide a customized solution for major corporations, but they present their own challenges if a company wants to adopt any type of technology requiring integration with existing ERP systems, said Whitmire.

"There's a major distinction between using a cloud-based ERP versus on-premise ERP, and really, in my opinion, that circles around the ability to integrate with it," he noted. "With the cloud-based ERP, there is a uniform API and companies are able to build integrations and sell to every client because of how consistent that integration practice is."

Those custom, in-house ERP systems, though, demand greater involvement from IT teams to support integrations from third-party service providers, Whitmire added.

"The inherent challenge is how customized the ERP is, and how bulky the implementation is for those larger clients," he said. "That's a big bottleneck for them."

FloQast specializes in helping businesses close the books, but when an enterprise is working with an in-house ERP system, there can be too many "cooks in the kitchen," according to Whitmire.

"When you have a team of people working on different aspects of your accounts, there are a lot of moving parts," he said. "They're booking journal entries and making adjustments to them, and the whole team is working in siloes when they need to be working together to produce an accurate financial statement."

One accountant may be working with revenue teams, while another is working with billing and invoicing. As each makes an adjustment to those journal entries, the rest of the finance team needs to know. Using data from in-house ERP systems makes it more difficult to keep everyone on the same page, Whitmire explained.

FloQast recently released a solution, Cloud Connect, that targets corporations using on-premise ERP systems. The tool enables finance teams to gain real-time access to the data stored in their ERPs via their existing cloud infrastructures.

Whitmire noted the tool uses robotics process automation to automate tedious, time-consuming tasks he said are "redundant" and "not difficult for a robot to figure out."

While the tool aims to save time, the executive also explained it was designed to keep accounting and finance professionals on the same page within the enterprise, helping as they all work toward a common goal that can sometimes be obscured when on-premise ERPs are deployed.

"Each side needs to understand when balances are changing," he explained. "You need to understand in real-time, or as close to real-time as possible, [if] those balances that [you've] been working on that change without my knowledge. It's purely a function of having a lot of cooks in the kitchen because we have a lot of work to do when closing the books, and a tight deadline to hit."

RELATED ITEMS: **API**, **B2B**, **B2B PAYMENTS**, **CLOUD ERP**, **CLOUD SOLUTIONS**, **CORPORATE ACCOUNTING**, **CORPORATE FINANCE**, **ENTERPRISE RESOURCE PLANNING**, **ERP**, **FINANCIAL DATA**, **FLOQAST**, **FLOQAST CLOUD CONNECT**, **IN HOUSE ERP**, **MIKE WHITMIRE**, **PAYMENTS**

B2B PAYMENTS

Despite Cybersecurity Standards, FIs Exposed To Third-Party Risks

By PYMNTS

Posted on October 2, 2017

Bank customers and regulators would likely agree: There's no excuse for a financial institution to accept lackluster cybersecurity measures. But according to a new report from BitSight, that's exactly what's happening as FIs work with partners and other third-party service providers.

Last week, the company published its latest report, "**The Buck Stops Where? Assessing the Cybersecurity Performance of the Finance Supply Chain**," which explores how financial service providers manage third-party cyber risk. Most of the time, BitSight concluded, banks and other FIs aren't holding their financial supply chains up to the same security standards as they hold themselves.

"While finance organizations tend to have more sophisticated vendor risk management programs, there is a lot of work to be done to close the performance gap between their own organizations and their immediate business ecosystem," explained BitSight Co-Founder and CEO Stephen Boyer in a **statement** announcing the research.

"The findings of this report are not only relevant for the finance sector but for companies across all industries who share with and rely upon external business services," he added. "Organizations should scrutinize the security culture and controls of their third and fourth parties. Ensuring that your vendor's systems are up to date and that their employees are not engaging in risky peer-to-peer file sharing is one way to reduce immediate third-party cyber risk."

In a survey of more than 5,200 legal, technology and business services organizations using the BitSight Security Rating Platform, the company explored how financial services companies are exposing themselves to the risk of cyberattacks because their immediate partners and members of their supply chain aren't adequately secured.

Analysts concluded that legal firms remain top performers when it comes to cybersecurity, while technology firms have some room to grow (though, researchers said, the tech sector has shown some improvement. Business services companies present the greatest cyber risk to their financial service partners.

PYMNTS takes a look at some of the key data points that reveal how banks are putting themselves at risk by not addressing the lapses in cybersecurity by their partners.

-20 percent of business services firms are still using Windows XP, while nearly the same portion of finance firms and technology companies are, too. Significant portions of these players are also still using Windows Vista. This is problematic, researchers warned, because Microsoft no longer supports Windows XP or Windows Vista, "and generally do not have security patches available to protect against new risks."

-Less than 10 percent of businesses analyzed received an 'A' grade for desktop software, with more than a third receiving the dreaded 'F' grade because their desktop software tools were outdated. Businesses that received a 'B' grade were more than twice as likely to have had some type of compromise of their systems in the last year, the research found. "This means that outdated desktop operating systems and browsers that exist within a supply chain are correlated to more immediate risks of machine compromise and data loss," the report concluded.

-23 percent of technology companies and 22 percent of business services firms have downloaded applications that lead to an increased likelihood of an unwanted application being inadvertently downloaded onto a network. Previous research from BitSight concluded that high levels of file sharing correlate with higher rates of system compromise.

According to BitSight, the cybersecurity lapses — largely from business services and financial companies — can present increased exposure to risk of cyberattacks to the financial institutions working with these companies.

"Third-party risks management is imperative today for organizations large and small," the report concluded. "Senior executives and Boards of Directors are increasingly asking for updates into their vendor risk management programs and looking for demonstrable progress in reducing third-party cyber risk."

"While finance organizations tend to have more sophisticated vendor risk management programs, there is much work to be done to close the performance gap between their own organizations and their immediate business ecosystems," BitSight added. "The finance of this report [is] not only relevant for the Finance sector; companies across all industries who share data and network access should place a great deal of security on the security culture of the third and fourth parties in their business ecosystem."

RELATED ITEMS: **B2B**, **B2B PAYMENTS**, **BITSIGHT**, **CYBERSECURITY**, **FINANCIAL SERVICES**, **NEWS**, **THIRD-PARTY RISK**

SHARE TWEET SHARE SHARE PRINT EMAIL

CASH

Why Cash Is King In Puerto Rico

By PYMNTS

Posted on October 2, 2017

Cash is king—and that is particularly true when it comes to helping victims of Hurricane Maria in Puerto Rico.

According to a **news report in CNBC**, citing the Voluntary Organizations Active in Disaster, those looking to help can do the most good by making cash donations. The organization's website states that many disaster relief organizations can't handle all the goods being shipped there in the early days of the recovery. The inability to handle the volume of donations is due to storage and sorting issues, as well as perishables spoiling as they wait to be distributed. Aid organizations are instead **recommending cash donations**, reported CNBC.

In many cases, a deluge of material goods creates "a second disaster," said Regine Webster, a vice president at the Center for Disaster Philanthropy, in the CNBC interview. "There are systems in place to get people what they need," she said, noting such mishaps as heavy coats being shipped to warn areas. Cash, on the other hand, can ensure that areas can obtain exactly what they need.

The report noted that through last Thursday, $295.3 million has been collected for the Harvey relief fund, with $98.3 million for Irma and $21.9 million for Maria.

Meanwhile, the Center for International Disaster Information provided 55 ways people can turn their goods into cash to send to Puerto Rico, including hosting a garage sale. What's more, a slew of charities are taking cash donations online, including Unicef, the American Red Cross and Save the Children. There's also United for Puerto Rico, a new relief effort created by the First Lady of Puerto Rico, Beatriz Rossello. It is backed by large companies, including Banco Popular, Coca-Cola, Burger King, Walmart, Walgreens, JetBlue and Bacardi. Global Giving, a crowdfunding website that set a goal of raising $5 million for Puerto Rico and the Caribbean, has collected $2.7 million from 22,803 people. The website matches donations to charities and groups in 170 countries, noted CNBC.